Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	68216	(encrypt$3 or encipher$3)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:10
S2	22197	S1 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:11
S3	328	S2 and ((signal or broadcast) with (random with (sequence or subsequence)))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:12
S4	4	("5003598" or "5161244").pn.	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:17
S5	42	S3 and ((subsequence or sequence or encrypt$3 or encipher$3 or key or random) with (reservoir or pool or database or file))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:21
S6	17	S5 and (count or counter)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:18
S7	17	S6 and time	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:42
S8	12	S7 and synchron$7	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 14:51

S9	1	S3 and ((subsequence or sequence or encrypt$3 or encipher$3 or key or random) with (reservoir or pool))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:21
S10	1	S7 and ((fill or full) with (value or count or counter))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:26
S11	33202	random adj (number or value)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:42
S12	15608	S11 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:42
S13	260	S12 and ((value or number) with (pool or reservoir))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:46
S14	23	S13 and ((fill or maintain) with (pool or reservoir))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:44
S15	1708	380/259-262,277-279.ccls.	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:47
S16	893	S15 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:47

S17	361	S16 and (random adj (number or value))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:48
S18	47	S17 and (select$3 with time) and synchron$7	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:49
S19	21	S18 and (time with (sequence or subsequence))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:51
S20	0	S19 and (key with (pool or reservoir))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:51
S21	42	S2 and (key with (pool or reservoir))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 10:51
S22	2	"5060266" .pn.	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:15
S23	95	("5201000" "6185316" "5870474" "6393484" "6424714" "5850450" "6252544" "6429812" "6301660" "6307938" "6345098" "5276737" "5315658" RE35808 RE36918 "5883956" "6282648" "6289453" "5412723" "5588056" "5850448" "6044388" "6104810" "5481610" "5517567" "5796830" "6052469" "6219421" "6219421" "4567600" "5592552" "6289314" "4323921" "4433207" "5442703" "5956404" "5535276" "5189700" "5737419" "5960086" "5604803" "5732137" "5777558" "5808607" "6091819" "6697488" "6760440" "5436972" "6141423" "6216229").pn.	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:15

S24	89	S23 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:17
S25	7	S24 and (reservoir or pool)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:47
S26	0	S24 and (reservoir)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:17
S27	183	(encrypt$3 or encipher$3) and ((key or (random adj number)) with (reservoir or pool))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:19
S28	59	S27 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:19
S29	169	(random adj number) with (reservoir or pool)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:47
S30	62	S29 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/19 15:47
S31	12006	(encrypt$3 or encipher$3) and ((time or period) with key)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 10:29

S32	4038	S31 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 10:31
S33	1360	S32 and (random adj (number or symbol))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 10:31
S34	240	S33 and ((select or choose) with (time or period))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 10:33
S35	59	S33 and ((select or choose) with (time or period) with key)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:01
S36	0	S35 and ((seed adj value) with random)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:01
S37	53	S33 and ((seed adj value) with random)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:02
S38	4	S33 and ((seed adj value) with random with (time or period))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:10
S39	4754	random adj time	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:11

S40	90	S39 and (seed adj (time or value or number))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:11
S41	35	S40 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:16
S42	5	S41 and (key with seed)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/20 11:16
S43	588	(random with (time or period or interval)) and (key with seed)	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/22 11:46
S44	218	S43 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/22 11:46
S45	16404	(encrypt$3 or encipher$3 or key or number) and ((reservoir or pool) with (threshold or fill or full))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/22 13:12
S46	1967	S45 and (("bit count" or "key count" or "n-bit" or "k-bit" or "bit" or "number") with (threshold or fill or full))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/22 13:13
S47	831	S46 and @ad<"19990716"	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/22 13:14

S48	244	S47 and ((key or number) with (creat$3 or generat$3))	US-PGPUB; USPAT; USOCR; EPO; DERWENT; IBM_TDB	OR	ON	2005/04/22 13:15

```
Set     Items    Description
S1         20    AU=REECE R?
S2     342931    RANDOM?
S3          2    S1 AND S2
```

1 3/9/1   (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

014385417   **Image available**
WPI Acc No: 2002-206120/200226
XRPX Acc No: N02-156972
  Data encryption/decryption method involves generating
  encryption/decryption subsequence from random **number sequence based on**
  private key, and both subsequences have identical boundary
Patent Assignee: REECE R W (REEC-I)
Inventor: **REECE R W**
Number of Countries: 020 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200209344	A1	20020131	WO 2001US22188	A	20010713	200226	B
EP 1310059	A1	20030514	EP 2001955834	A	20010713	200333	
			WO 2001US22188	A	20010713		

Priority Applications (No Type Date): US 2000617913 A 20000717
Patent Details:
Patent No Kind Lan Pg   Main IPC   Filing Notes
WO 200209344 A1 E   76 H04L-009/00
    Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU
    MC NL PT SE TR
EP 1310059   A1 E   H04L-009/00   Based on patent WO 200209344
    Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI
    LU MC NL PT SE TR

Abstract (Basic): WO 200209344 A1
    NOVELTY - A plain text data is encrypted using private key and
  encryption subsequence, which is selected from the **random** number
  sequence with respect to private key. A decryption subsequence is
  selected from **random** number sequence based on the private key. The
  boundaries of the decryption and encryption subsequence are identical.
  The encrypted data is decrypted using the subsequence and the key.
    USE - For encryption and decryption of plain text data for
  broadcasting applications, military applications using GPS, and also
  for electronic-commerce.
    ADVANTAGE - The encrypted messages are exchanged between the user
  with very low risk and improved safety.
    DESCRIPTION OF DRAWING(S) - The figure explains the system block
  diagram of the encryption/decryption method.
    pp; 76 DwgNo 1/9

```
File 696:DIALOG Telecom. Newsletters 1995-2005/Apr 20
        (c) 2005 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2005/Apr 21
        (c) 2005 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2004/Dec
        (c) 2005 The HW Wilson Co.
File 112:UBM Industry News 1998-2004/Jan 27
        (c) 2004 United Business Media
File 141:Readers Guide 1983-2005/Dec
        (c) 2005 The HW Wilson Co
File 484:Periodical Abs Plustext 1986-2005/Apr W3
        (c) 2005 ProQuest
File 608:KR/T Bus.News. 1992-2005/Apr 21
        (c)2005 Knight Ridder/Tribune Bus News
File 813:PR Newswire 1987-1999/Apr 30
        (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2005/Apr 21
        (c) 2005 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2005/Apr 21
        (c) 2005 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
        (c) 1999 Business Wire
File 610:Business Wire 1999-2005/Apr 21
        (c) 2005 Business Wire.
File 369:New Scientist 1994-2005/Mar W3
        (c) 2005 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
        (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2005/Apr 21
        (c) 2005 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2005/Apr 21
        (c) 2005 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2005/Apr 20
        (c) 2005 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2005/Apr W1
        (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Apr W3
        (c) 2005 IDG Communications
```

Set	Items	Description
S1	4425797	KEY? ? OR ALGORITHM? OR CIPHER? ? OR CYPHER? ? OR SUBKEY? ? OR SUBCIPHER? OR SUBCYPHER? ?
S2	7094498	SECURITY OR SECRET OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR CRYPTO OR CRYPTOL? OR CRYPTOGRAPH? OR CRYPTANALY? OR CRYPTOS-YSTEM?
S3	20	SECRETKEY? OR PRIVATEKEY? OR CRYPTOKEY?
S4	126770	ENCOD??? ? OR INCOD??? ?
S5	858895	SAMPL?
S6	1145253	INTERVAL? OR TIMEFRAME? OR TIMING OR TIMECYCLE? OR DURATIO-N? OR TIMESPAN?
S7	17587252	TIME OR TIMES
S8	4750678	PERIOD? ?
S9	467156	S6:S8(3N)(START? OR BEGIN? OR INITIAT? OR SELECT???? ?)
S10	118577	S6:S8(3N)(SPECIFIE? ? OR SPECIFICATION? OR SPECIFY? OR DES-IGNAT? OR STIPULAT? OR IDENTIFY? OR IDENTIFIE? ? OR IDENTIFIC-ATION?)
S11	102948	S6:S8(3N)(CHOOS? OR CHOSE? ? OR DEFIN?)
S12	356140	S6:S8(3N)(BASE? ? OR BASING OR DETERMIN? OR CALCULAT? OR D-ET? ? OR DERIV? OR GENERAT???? ? OR CALIBRAT? OR TABULAT? OR -ASCERTAIN?)
S13	17159	S6:S8(3N)(COMPUTAT? OR COMPUTING OR COMPUTE OR COMPUTES OR

```
                 COMPUTED)
S14    153279   S6:S8(3N)(INTERPOLAT? OR ESTIMAT? OR APPROXIMAT?)
S15     30405   (S2 OR S4)(2W)S1 OR PRIVATE(2W)S1 OR S3
S16      8235   S9:S11(10N)S12:S14
S17      4592   S5(5N)S9:S14
S18         4   S15(S)S16:S17
S19         1   S18/2000:2005
S20         3   S18 NOT S19
S21         2   RD (unique items)
? t21/k/all
```

21/K/1   (Item 1 from file: 813)
DIALOG(R)File 813:(c) 1999 PR Newswire Association Inc. All rts. reserv.

... a wide array of security requirements, SafeNet includes the full suite
of Internet security -- user **identification** , one- **time** password
 generation   , access control, data encryption, and packet authentication.
Unlike competing solutions, SafeNet allows critical network security
functions, such as **encryption key** management, to be controlled either
in the user environment or outsourced to the security experts...

21/K/2   (Item 1 from file: 613)
DIALOG(R)File 613:(c) 2005 PR Newswire Association Inc. All rts. reserv.

...Gerlach, VP and Chief Engineer, says, "When you buy the system, you
get a specially **encoded** wireless electronic **key** and a small
undetectable
electronic 'tag' you attach to your car. The tag is virtually...

...probable theft and an alert is transmitted to the Centraxx monitoring
center
by the nearest **base** station. Dynamic real **time** tracking is **initiated**
immediately and the police are notified enabling prompt recovery."

    He added, "The real beauty of...
?

File   9:Business & Industry(R) Jul/1994-2005/Apr 20
          (c) 2005 The Gale Group
File   16:Gale Group PROMT(R) 1990-2005/Apr 20
          (c) 2005 The Gale Group
File   47:Gale Group Magazine DB(TM) 1959-2005/Apr 21
          (c) 2005 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2005/Apr 21
          (c)2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
          (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2005/Apr 21
          (c) 2005 The Gale Group
File 570:Gale Group MARS(R) 1984-2005/Apr 21
          (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Apr 21
          (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Apr 21
          (c) 2005 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2005/Apr 08
          (c) 2005 The Gale Group

Set   Items   Description
S1   4250116   KEY? ? OR ALGORITHM? OR CIPHER? ? OR CYPHER? ? OR SUBKEY? ?
                 OR SUBCIPHER? OR SUBCYPHER? ?
S2   2900563   SECURITY OR SECRET OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
                 CRYPTO OR CRYPTOL? OR CRYPTOGRAPH? OR CRYPTANALY? OR CRYPTOS-
                 YSTEM?
S3   14   SECRETKEY? OR PRIVATEKEY? OR CRYPTOKEY?
S4   163905   ENCOD??? ? OR INCOD??? ?
S5   1617140   SAMPL?
S6   14820428   TIME OR TIMES OR PERIOD? OR INTERVAL? OR TIMEFRAME? OR TIM-
                 ING OR TIMECYCLE? OR DURATION? OR TIMESPAN?
S7   382378   S6(3N)(START? OR BEGIN? OR INITIAT? OR SELECT???? ?)
S8   113157   S6(3N)(SPECIFIE? ? OR SPECIFICATION? OR SPECIFY? OR DESIGN-
                 AT? OR STIPULAT? OR IDENTIFY? OR IDENTIFIE? ? OR IDENTIFICATI-
                 ON?)
S9   84407   S6(3N)(CHOOS? OR CHOSE? ? OR DEFIN?)
S10   376453   S6(3N)(BASE? ? OR BASING OR DETERMIN? OR CALCULAT? OR DET?
                 ? OR DERIV? OR GENERAT???? ? OR CALIBRAT? OR TABULAT? OR ASCE-
                 RTAIN?)
S11   156717   S6(3N)(INTERPOLAT? OR ESTIMAT? OR APPROXIMAT?)
S12   23494   S6(3N)(COMPUTAT? OR COMPUTING OR COMPUTE OR COMPUTES OR CO-
                 MPUTED)
S13   47444   (S2 OR S4)(2W)S1 OR PRIVATE(2W)S1 OR S3
S14   9067   S10:S12(10N)S7:S9
S15   4464   S5(5N)S7:S12
S16   6   S13(S)S14:S15
S17   4   S16/2000:2005
S18   2   S16 NOT S17
S19   2   RD (unique items)

 19/K/1   (Item 1 from file: 16)
DIALOG(R)File   16:(c) 2005 The Gale Group. All rts. reserv.

...   on the gains. Money outside of an annuity is not 100%
reinvestable.'
     Distributions And Social **Security** Benefits
     A **key** part of the post-retirement planning strategy involves
determining the best **time** to **begin** taking distributions and receiving
Social Security benefits. When to begin drawing down retirement assets can
...

Set	Items	Description
S1	2879067	KEY? ? OR ALGORITHM? OR CIPHER? ? OR CYPHER? ? OR SUBKEY? ? OR SUBCIPHER? OR SUBCYPHER? ?
S2	646621	SECURITY OR SECRET OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR CRYPTO OR CRYPTOL? OR CRYPTOGRAPH? OR CRYPTANALY? OR CRYPTOSYSTEM?
S3	4	SECRETKEY? OR PRIVATEKEY? OR CRYPTOKEY?
S4	481367	ENCOD??? ? OR INCOD??? ?
S5	2994881	SAMPL?
S6	10805191	TIME OR TIMES OR PERIOD? OR INTERVAL? OR TIMEFRAME? OR TIMING OR TIMECYCLE? OR DURATION? OR TIMESPAN?
S7	116347	S6(3N)(START? OR BEGIN? OR INITIAT? OR SELECT???? ?)
S8	73894	S6(3N)(SPECIFIE? ? OR SPECIFICATION? OR SPECIFY? OR DESIGNAT? OR STIPULAT? OR IDENTIFY? OR IDENTIFIE? ? OR IDENTIFICATION?)
S9	54551	S6(3N)(CHOOS? OR CHOSE? ? OR DEFIN?)
S10	492424	S6(3N)(BASE? ? OR BASING OR DETERMIN? OR CALCULAT? OR DET? ? OR DERIV? OR GENERAT???? ? OR CALIBRAT? OR TABULAT? OR ASCERTAIN?)
S11	228206	S6(3N)(INTERPOLAT? OR ESTIMAT? OR APPROXIMAT?)
S12	119405	S6(3N)(COMPUTAT? OR COMPUTING OR COMPUTE OR COMPUTES OR COMPUTED)
S13	21693	(S2 OR S4)(2W)S1 OR PRIVATE(2W)S1 OR S3
S14	12923	S10:S12(10N)S7:S9

```
S15      16631   S5(5N)S7:S12
S16          6   S13 AND S14:S15
S17          3   S16/2000:2005
S18          3   S16 NOT S17
S19          3   RD (unique items)
```

19/7/1   (Item 1 from file: 2)
DIALOG(R)File   2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

03782986   INSPEC Abstract Number: B91003780
 Title: A secret key **cryptosystem using a chaotic map**
  Author(s): Habutsu, T.; Nishio, Y.; Sasase, I.; Mori, S.
  Author Affiliation: Fac. of Sci. & Technol., Keio Univ., Yokohama, Japan
  Journal: Transactions of the Institute of Electronics, Information and
Communication Engineers E   vol.E73, no.7   p.1041-4
  Publication Date: July 1990 Country of Publication: Japan
  CODEN: TIEEEV ISSN: 0913-574X
  Language: English   Document Type: Journal Paper (JP)
  Treatment: New Developments (N); Practical (P); Theoretical (T)
  Abstract: Proposes a new **secret** **key** cryptosystem using a chaotic map.
This system is based on the characteristics of chaos that the small
variations of parameters make the results of recursive calculations on
chaotic maps quite different. By appropriately setting the **calculation**
 times and **selecting** a parameter as a **secret** **key**, one can make a
useful cryptosystem whose distribution of ciphertexts is uniform
distribution U(01,) and the results of the computation for two slightly
different keys are relatively independent. (4 Refs)
  Subfile: B

19/7/3   (Item 1 from file: 94)
DIALOG(R)File   94:JICST-EPlus
(c)2005 Japan Science and Tech Corp(JST). All rts. reserv.

01182260   JICST ACCESSION NUMBER: 91A0042656   FILE SEGMENT: JICST-E
Special issue on cryptography and information security . A secret   key
   cryptosystem using a chaotic map.
HABUTSU T (1); NISHIO Y (1); SASASE I (1); MORI S (1)
(1) Keio Univ., Yokohama-shi, JPN
Trans Inst Electron Inf Commun Eng E, 1990, VOL.73,NO.7, PAGE.1041-1044,
   FIG.5, REF.4
JOURNAL NUMBER: F0699BBZ   ISSN NO: 0387-236X
UNIVERSAL DECIMAL CLASSIFICATION: 621.391
LANGUAGE: English   COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: In this paper we propose a new **secret** **key** cryptosystem using
   a chaotic map. This system is based on the characteristics of chaos
   that the small variations of parameters make the results of recursive
   calculations on chaotic maps quite different. By appropriately setting
   the **calculation** **times** and **selecting** a parameter as a **secret**
   key, we can make a useful cryptosystem whose distribution of
   ciphertexts is uniform distribution U(0,1) and the results of the
   computation for two slight different keys are relatively
   independent.(author abst.)
?

File 347:JAPIO Nov 1976-2004/Dec(Updated 050405)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200525
        (c) 2005 Thomson Derwent
File 344:Chinese Patents Abs Aug 1985-2004/May
        (c) 2004 European Patent Office
File 371:French Patents 1961-2002/BOPI 200209
        (c) 2002 INPI. All rts. reserv.

Set   Items   Description
S1   274789   KEY? ? OR ALGORITHM? OR CIPHER? ? OR CYPHER? ? OR SUBKEY? ?
                 OR SUBCIPHER? OR SUBCYPHER? ?
S2   110349   SECURITY OR SECRET OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
                 CRYPTO OR CRYPTOL? OR CRYPTOGRAPH? OR CRYPTANALY? OR CRYPTOS-
                 YSTEM?
S3   10   SECRETKEY? OR PRIVATEKEY? OR CRYPTOKEY?
S4   194886   ENCOD??? ? OR INCOD??? ?
S5   391245   SAMPL?
S6   3784977   TIME OR TIMES OR PERIOD? OR INTERVAL? OR TIMEFRAME? OR TIM-
                 ING OR TIMECYCLE? OR DURATION? OR TIMESPAN?
S7   144277   S6(3N)(START? OR BEGIN? OR INITIAT? OR SELECT???? ?)
S8   75951   S6(3N)(SPECIFIE? ? OR SPECIFICATION? OR SPECIFY? OR DESIGN-
                 AT? OR STIPULAT? OR IDENTIFY? OR IDENTIFIE? ? OR IDENTIFICATI-
                 ON?)
S9   19090   S6(3N)(CHOOS? OR CHOSE? ? OR DEFIN?)
S10   280424   S6(3N)(BASE? ? OR BASING OR DETERMIN? OR CALCULAT? OR DET?
                 ? OR DERIV? OR GENERAT???? ? OR CALIBRAT? OR TABULAT? OR ASCE-
                 RTAIN?)
S11   19021   S6(3N)(INTERPOLAT? OR ESTIMAT? OR APPROXIMAT?)
S12   13242   S6(3N)(COMPUTAT? OR COMPUTING OR COMPUTE OR COMPUTES OR CO-
                 MPUTED)
S13   11906   (S2 OR S4)(2W)S1 OR PRIVATE(2W)S1 OR S3
S14   18392   S10:S12(10N)S7:S9
S15   7884   S5(5N)S7:S12
S16   8   S13 AND S14:S15
S17   8   IDPAT (sorted in duplicate/non-duplicate order)
S18   8   IDPAT (primary/non-duplicate records only)

 18/9/2   (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

014865187   **Image available**
WPI Acc No: 2002-685893/200274
XRPX Acc No: N02-541478
  Key generation device e.g. for elliptical curvilinear encryption ,
  chooses key **generation system based on key selection limit, maximum key
  bit length and** time **for** calculation specified **by user for
  generating the key**
Patent Assignee: TOSHIBA KK (TOKE)
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No   Kind   Date   Applicat No   Kind   Date   Week
JP 2002207425 A   20020726 JP 20014043   A   20010111 200274 B

Priority Applications (No Type Date): JP 20014043 A 20010111
Patent Details:
Patent No Kind Lan Pg   Main IPC   Filing Notes
JP 2002207425 A   17 G09C-001/00

Abstract (Basic): JP 2002207425 A

```
File 348:EUROPEAN PATENTS 1978-2005/Apr W02
        (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050414,UT=20050407
        (c) 2005 WIPO/Univentio
File 324:German Patents Fulltext 1967-200515
        (c) 2005 Univentio


Set     Items    Description
S1      377907   KEY? ? OR ALGORITHM? OR CIPHER? ? OR CYPHER? ? OR SUBKEY? ?
                 OR SUBCIPHER? OR SUBCYPHER? ?
S2      231115   SECURITY OR SECRET OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
                 CRYPTO OR CRYPTOL? OR CRYPTOGRAPH? OR CRYPTANALY? OR CRYPTOS-
                 YSTEM?
S3         121   SECRETKEY? OR PRIVATEKEY? OR CRYPTOKEY?
S4      186878   ENCOD??? ? OR INCOD??? ?
S5      542880   SAMPL?
S6     2457171   TIME OR TIMES OR PERIOD? OR INTERVAL? OR TIMEFRAME? OR TIM-
                 ING OR TIMECYCLE? OR DURATION? OR TIMESPAN?
S7      209576   S6(3N)(START? OR BEGIN? OR INITIAT? OR SELECT???? ?)
S8       87616   S6(3N)(SPECIFIE? ? OR SPECIFICATION? OR SPECIFY? OR DESIGN-
                 AT? OR STIPULAT? OR IDENTIFY? OR IDENTIFIE? ? OR IDENTIFICATI-
                 ON?)
S9       73444   S6(3N)(CHOOS? OR CHOSE? ? OR DEFIN?)
S10     316738   S6(3N)(BASE? ? OR BASING OR DETERMIN? OR CALCULAT? OR DET?
                 ? OR DERIV? OR GENERAT???? ? OR CALIBRAT? OR TABULAT? OR ASCE-
                 RTAIN?)
S11      97375   S6(3N)(INTERPOLAT? OR ESTIMAT? OR APPROXIMAT?)
S12      29307   S6(3N)(COMPUTAT? OR COMPUTING OR COMPUTE OR COMPUTES OR CO-
                 MPUTED)
S13     549257   SAMPL???? ?
S14      17250   S2:S4(2W)S1
S15      30858   (S10:S12 OR S6(3N)(DERIV??? ? OR DERIVATION?))(10N)(S7:S9 -
                 OR S6(3N)DEFIN??? ?)
S16      18537   S13(5N)S7:S12
S17       1740   S13(5N)(S6(3N)(DERIV??? ? OR DERIVATION?) OR S6(3N)DEFIN???
                 ?)
S18         30   S14(20N)S15:S17
S19         30   IDPAT (sorted in duplicate/non-duplicate order)
S20         29   IDPAT (primary/non-duplicate records only)
S21       6134   PRIVATE(2W)S1 OR S3
S22         12   S21(20N)S15:S17 NOT S18
S23         12   IDPAT (sorted in duplicate/non-duplicate order)
S24         12   IDPAT (primary/non-duplicate records only)
```